DOCID: 4165173

NATIONAL SECURITY AGENCY
CENTRAL SECURITY SERVICE
FORT GEORGE G. MEADE, MARYLAND 20755-6000

This date should read 13 February 2009. → 13 February 2008

MEMORANDUM FOR THE ASSISTANT TO THE SECRETARY OF DEFENSE (INTELLIGENCE OVERSIGHT)

SUBJECT: (U//~~FOUO~~) Required Actions for the CY 2008 Intelligence Oversight Report to Congress – INFORMATION MEMORANDUM

(U//~~FOUO~~) In accordance with your memorandum of 4 December 2008, the enclosed consolidation of the National Security Agency's Quarterly Reports to the President's Intelligence Oversight Board for calendar year 2008 is provided to assist the Secretary of Defense in preparation of his Annual Report to Congress.

George Ellard

GEORGE ELLARD
Inspector General

Encl:
Annual Report

This document may be declassified and marked "UNCLASSIFIED//~~For Official Use Only~~" upon removal of enclosure(s)

Approved for Release by NSA on 12-19-2014, FOIA Case # 70809 (Litigation)

Derived From: NSA/CSSM 1-52
Dated: 20070108
Declassify On: 20320108

1. (U//~~FOUO~~) Intelligence, counterintelligence, and intelligence-related activities that violate law, regulation, or policy substantiated during the quarter, as well as actions taken as a result of the violations.

(U) Intelligence Activities

~~(TS//SI//REL TO USA, AUS, CAN, GBR, NZL)~~ **Unintentional collection against United States persons.** [redacted] instances in which Signals Intelligence (SIGINT) analysts inadvertently collected communications to, from, or about United States (U.S.) persons while pursuing foreign intelligence tasking were reported in 2008. Unless otherwise noted, all intercepts and reports have been deleted or destroyed as required by United States SIGINT Directive (USSID) SP0018.

(b)(1)
(b)(3)-P.L. 86-36

(U) Unauthorized Targeting

(b)(1)
(b)(3)-P.L. 86-36
(b)(3)-50 USC 3024(i)

~~(TS//SI//NF)~~ A National Security Agency/Central Security Service (NSA/CSS) analyst tasked the telephone numbers associated with a U.S. [redacted] without verifying that consent for collection had been given by the [redacted] and approved by the Director of NSA. The selectors, on coverage [redacted] were detasked. [redacted] intercepts were purged from data repositories on [redacted] when the mistake was found during a target review.

~~(S//REL TO USA, FVEY)~~ A software problem resulted in collection on a [redacted] beginning [redacted] The software, [redacted] was turned off [redacted] when the violation was recognized. It was returned to service [redacted] after the problem was diagnosed, corrected, and tested. All related collection was purged from the database and related analysis tool.

(b)(1)
(b)(3)-P.L. 86-36

(b)(1)
(b)(3)-P.L. 86-36
(b)(3)-50 USC 3024(i)

~~(S//SI//REL TO USA, FVEY)~~ [redacted] were inadvertently targeted during [redacted] Unknown to the system testers, the [redacted] selectors were owned by a U.S. [redacted] The analysts removed the [redacted] from the query and checked the remaining selectors to avoid future testing mistakes on [redacted]

~~(TS//SI//REL TO USA, FVEY)~~ [redacted]

~~(TS//SI//NF)~~ [redacted]

(b)(1)
(b)(3)-P.L. 86-36
(b)(3)-18 USC 798
(b)(3)-50 USC 3024(i)

Derived From: NSA/CSSM 1-52
Dated: 20070108
Declassify On: 20320108

(b)(1)
(b)(3)-P.L. 86-36
(b)(3)-50 USC 3024(i)
USC 798

(b)(1)
(b)(3)-P.L. 86-36

~~(TS//SI//NF)~~ prior to approved consensual collection, an NSA analyst queried on a U.S. telephone number retroactively The analyst did not understand he could not search for data prior to the consensual collection authorization date. The query and results were deleted the same day.

(b)(1)
(b)(3)-P.L. 86-36

~~(S//SI//NF)~~ an NSA/CSS analyst targeted a foreign person in the United States without AG authorization. She learned that a person tied to the was in the United States and was suspected to have planned an operation to take place Thinking only of the urgency and not the target's location, the analyst queried an NSA database for information without seeking authorization to target the individual. No results were returned. The incident was found by the analyst's auditor, and the analyst was counseled and received remedial training.

(b)(1)
(b)(3)-P.L. 86-36
(b)(3)-18 USC 798

~~(TS//SI//NF)~~ An oversight resulted in the continued targeting of a U.S. person after his consent to monitoring expired. Although the consent expired NSA/CSS analysts did not remove the selector from collection until There were resulting intercepts were purged from NSA databases.

(b)(1)
(b)(3)-P.L. 86-36
(b)(3)-18 USC 798
(b)(3)-50 USC 3024(i)

~~(TS//SI//NF)~~ An NSA/CSS analyst tasked collection on a U.S. person before receiving AG authorization on The analyst wrongly believed that authorization had been received. The unauthorized action resulted in the intercept of between All collected data was purged when the violation was discovered and no reports were issued on the data.

(b)(1)
(b)(3)-P.L. 86-36
(b)(3)-18 USC 798

(b)(1)
(b)(3)-P.L. 86-36

~~(TS//SI//REL TO USA, FVEY)~~ the used the U.S. SIGINT System to locate a believed to be kidnapped The selectors were tasked before authorization was obtained from NSA. After the NSA OGC denied the authorization request, the was found. He had not been kidnapped. The responsible analysts have received additional intelligence oversight training.

(b)(1)
(b)(3)-P.L. 86-36
(b)(3)-18 USC 798
(b)(3)-50 USC 3024(i)

~~(TS//SI//NF)~~ An NSA analyst incorrectly tasked a U.S. telephone number for collection on He assumed that the selector was foreign because foreign intelligence target. This mistake was found during a review of tasked selectors on The selector was detasked the same day. The analyst was paired with a senior analyst for additional training. No collection resulted from this violation.

~~(TS//SI//NF)~~ A selector for an AG-authorized target remained on collection for nine days after the AG authorization expired on The selector was detasked on

(b)(1)
(b)(3)-P.L. 86-36

(b)(1)
(b)(3)-P.L. 86-36

No collection occurred as a result of the process violation. A review of all targeted selectors related to the target confirmed they had been terminated on or before

~~(TS//SI//REL TO USA, FVEY)~~ On occasions between analysts incorrectly entered their own information into an NSA database for SIGINT collection and analysis. Believing that the data field required information on the analyst who tasked the selectors, the analysts entered their When the mistake was identified on the data was removed, and the analysts received additional tasking training.

(b)(1)
(b)(3)-P.L. 86-36

~~(TS//SI//REL TO USA, FVEY)~~

(b)(1)
(b)(3)-P.L. 86-36
(b)(3)-50 USC 3024(i)
(b)(3)-18 USC 798

~~(TS//SI//REL TO USA, FVEY)~~ an NSA analyst mistakenly targeted belonging to a instead of the associated with a foreign target. The violation was corrected by the analyst on and the associated collection was purged from the NSA database.

(b)(1)
(b)(3)-P.L. 86-36

~~(TS//SI//NF)~~ selectors were detasked and collection was destroyed when NSA suspected that a foreign target might be a U.S. person. An analyst misunderstood the direction to treat the target as a U.S. person until the target's and retasked the selectors The selectors were again detasked and intercept purged from NSA databases when the violation was identified

~~(TS//SI//REL TO USA, FVEY)~~ an NSA analyst improperly searched for information on eight NSA analysts to acquire translation metrics for their performance appraisals. the violation was found by a database auditor, who provided additional training to the analyst. The queries returned results, which were purged from the NSA database

(b)(1)
(b)(3)-P.L. 86-36

(U) U.S. Person Status

~~(S//SI//REL)~~ On occasions, targets initially thought to be legitimate and foreign were found to hold U.S. citizenship or permanent resident status. In instances, intercepts were retained and reported as authorized by USSID SP0018. The remaining collection was deleted from the database for audio, pre-release transcripts. Additionally, on occasions, targets the United States. Another legitimate foreign target in the United States. In all instances, the collection was terminated.

(b)(1)
(b)(3)-P.L. 86-36

~~(TS//SI)~~ On occasions, targeted were used by persons a U.S. person

(b)(1)
(b)(3)-P.L. 86-36
(b)(3)-50 USC 3024(i)

(b)(1)
(b)(3)-P.L. 86-36
(b)(3)-50 USC 3024(i)

(b)(1)
(b)(3)-P.L. 86-36
(b)(3)-18 USC 798

indicated use by . In instances, the numbers were removed from tasking and the intercept was deleted.

(b)(1)
(b)(3)-P.L. 86-36

~~(TS//SI//REL TO USA, FVEY)~~ No reports were issued on the intercept.

~~(S//SI)~~

(b)(1)
(b)(3)-P.L. 86-36
(b)(3)-18 USC 798
(b)(3)-50 USC 3024(i)

~~(TS//SI//NF)~~ , NSA/CSS analysts targeted U.S. persons the analyst searched for a U.S. in a raw traffic database because he did not realize that the was owned by the analyst did not follow research procedures, which required him to check occurred when another analyst failed to review Queries were terminated, and results were not retained. mistakes were found during the auditing and oversight functions, and the analysts were retrained on search procedures.

(b)(1)
(b)(3)-P.L. 86-36

~~(TS//SI//NF)~~ Transcription revealed that a was used by a U.S. The transcript noted a conversation between two U.S. When NSA/CSS learned of the incidental collection, minimization procedures were applied as directed by the USSID SP0018.

(b)(1)
(b)(3)-P.L. 86-36
(b)(3)-50 USC 3024(i)

~~(TS//SI//NF)~~

(b)(1)
(b)(3)-P.L. 86-36
(b)(3)-18 USC 798
(b)(3)-50 USC 3024(i)

~~(S//SI//REL TO USA, FVEY)~~ , a valid foreign target the United States. Tasking was terminated, and collection was purged from NSA databases. No reports were issued.

(b)(1)
(b)(3)-P.L. 86-36

~~(TS//SI//NF)~~ On occasions, targets initially thought to be legitimate and foreign were found to hold U.S. citizenship. , NSA terminated targeting when the relayed that the target held a U.S. passport. Collection was purged from databases, and reports were cancelled. selector was not detasked when U.S. person status was suspected. The detasking failure resulted in intercepts between when the selectors were positively linked to an The selectors were detasked, collection was purged and NSA/CSS analysts were retrained on the process for vetting inadvertent collection.

(b)(3)-P.L. 86-36

(b)(1)
(b)(3)-P.L. 86-36

(b)(1)
(b)(3)-P.L. 86-36
(b)(3)-18 USC 798
(b)(3)-50 USC 3024(i)

~~(TS//SI//NF)~~ during an NSA analysts collected communications from a target in the United States. The analysts failed to confirm the target's location prior to the collection. The messages were deleted when the error was identified.

(b)(1)
(b)(3)-P.L. 86-36

(U) Poorly Constructed Database Queries

~~(S//SI//REL)~~ There were instances of unintentional collection caused by poorly constructed database queries. All results were deleted from the storage system. Addtionally, NSA analysts improperly queried selectors in NSA databases on occasions during 2008.

~~(TS//SI//REL TO USA, FVEY)~~ On of the occasions, NSA analysts failed to verify that targets were located outside the United States before conducting database queries. In of the instances, the oversights resulted in metadata collection. No data was retrieved. All queries were terminated and when collection occurred, the data was deleted. No reports were issued.

(b)(1)
(b)(3)-P.L. 86-36

~~(S//SI//REL TO USA, FVEY)~~ During an audit of database queries, an auditor found that a junior analyst queried the of a U.S. person the analyst queried the a foreign intelligence target. She had not considered the possibility that the a U.S. person. No collection resulted from the query. The analyst received additional training on intelligence oversight authorities from her auditor.

~~(S//SI//REL TO USA, FVEY)~~ an NSA database auditor found that an analyst queried The queries and results were deleted, and the analyst enrolled in refresher training.

(b)(1)
(b)(3)-P.L. 86-36
(b)(3)-18 USC 798
(b)(3)-50 USC 3024(i)

(b)(1)
(b)(3)-P.L. 86-36

~~(TS//SI//NF)~~ On occasions during training courses or research, NSA analysts queried the of other analysts. In both cases, no results were returned. The analysts were instructed on proper query construction.

~~(TS//SI//NF)~~ an NSA mistakenly included the e-mail address of in a query list of targeted addresses. The analyst noticed his mistake the same day, and the query was terminated with no results on

(b)(1)
(b)(3)-P.L. 86-36
(b)(3)-50 USC 3024(i)

(U) Detasking Delays

~~(TS//SI//REL)~~ an NSA analyst learned that a targeted foreign e-mail account the United States on Detasking was not accomplished until This -day delay was the result of human error. The analyst did not read the status report containing the detasking request. There was no collection between

(b)(1)
(b)(3)-P.L. 86-36

(b)(1)
(b)(3)-P.L. 86-36
(b)(3)-50 USC 3024(i)

~~(TS//SI//REL TO USA, FVEY)~~ Not all of the selectors attributed to a target were [redacted] when NSA analysts [redacted] the United States. Target activity in the United States [redacted] Selectors were removed from collection systems [redacted] and [redacted] telephone calls were deleted [redacted]

~~(S//SI//NF)~~ [redacted] an NSA analyst removed [redacted] selectors of [redacted] but failed to detask the telephone numbers. The process failure was corrected on [redacted] when the error was identified. There was no collection from [redacted]

(b)(1)
(b)(3)-P.L. 86-36

~~(TS//SI//REL TO USA, FVEY)~~ [redacted] the United States on [redacted] selectors attributed to a target were detasked [redacted]; however, one collection site did not detask [redacted] e-mail selectors. The intercept associated with the [redacted] visit to the United States was purged from NSA databases on [redacted]

~~(S//SI//REL TO USA, FVEY)~~ [redacted] a target initially thought to be legitimate and foreign was found to be a U.S. citizen. Although queries were terminated and selectors were detasked, collection was not purged from NSA databases in a timely manner. Purging took place 11 days after the selector was detasked, when the analyst returned from sick leave.

(b)(1)
(b)(3)-P.L. 86-36

~~(TS//SI//REL TO USA, FVEY)~~ [redacted] an NSA analyst found [redacted] selectors that should have been detasked when NSA learned the target was a U.S. person. When the target's U.S. person status was discovered in early 2008, the telephone selectors were detasked, but the [redacted] selectors had been overlooked. No queries on the selectors had been made before [redacted] when the selectors were deleted, and all collection was purged from the database.

(b)(1)
(b)(3)-P.L. 86-36
(b)(3)-50 USC 3024(i)

(b)(1)
(b)(3)-P.L. 86-36

~~(TS//SI//NF)~~ [redacted] during routine oversight, an NSA database auditor found [redacted] telephone selectors [redacted] in the United States from [redacted] According to the analyst responsible for the query, [redacted] This process violation resulted in collection. The selectors were removed from the query, and collection was deleted on [redacted]

(b)(1)
(b)(3)-P.L. 86-36
(b)(3)-50 USC 3024(i)

~~(S//SI//REL TO USA, FVEY)~~ [redacted] a review of a [redacted] found that selectors for [redacted] foreign intelligence targets were not detasked [redacted] The selectors were detasked and collection between [redacted] was purged from NSA databases on [redacted]

~~(TS//SI//NF)~~ A valid foreign target traveled to the United States and [redacted] before the associated selector was detasked. A detasking request was submitted [redacted] visit to the United States. The detasking did not occur until [redacted] after the target returned overseas. This violation was caused by [redacted] for detasking. To lessen the risk of future violations of this type, analysts are now required to [redacted]

(b)(1)
(b)(3)-P.L. 86-36

(b)(1)
(b)(3)-P.L. 86-36

Collection associated with this violation was purged from NSA databases.

~~(TS//SI//REL TO USA, FVEY)~~ On two occasions, collection occurred while valid foreign targets were in the United States. In the first instance, detasking was requested but the selectors were not removed from All related collection was purged from NSA databases. The second instance occurred on Selectors were deactivated from when the target the United States, but collection occurred before detasked the selectors. The intercepts were purged from an NSA database as they were identified between No reporting resulted from either violation.

(b)(1)
(b)(3)-P.L. 86-36
(b)(3)-50 USC 3024(i)

~~(TS//SI//REL)~~ an NSA analyst learned that foreign targets were the United States targeted e-mail selectors were detasked, and collection for that day was purged from an NSA database. When confirming the detasking the analyst found that the selectors had not been removed from The cause of the problem was software-related. The selectors were No collection resulted had not been conducted from

(b)(1)
(b)(3)-P.L. 86-36

(b)(3)-P.L. 86-36

(U//~~FOUO~~) **Destruction Delays.** In instances, NSA analysts were not timely in removing SIGINT collection from NSA databases.

(b)(1)
(b)(3)-P.L. 86-36
(b)(3)-50 USC 3024(i)

~~(TS//SI//NF)~~ inadvertent intercepts collected on were purged from one database, but the analyst forgot to purge the data from a second database. The NSA analysis and production staff found the oversight on at which time the collection was deleted. The analyst reviewed the procedures for purging collection to lessen the possibility of a recurrence of a retention violation.

(b)(1)
(b)(3)-P.L. 86-36

~~(TS//SI//NF)~~ On occasions, NSA/CSS analysts did not purge unintentional collection from NSA databases in a timely manner. an e-mail selector for a legitimate foreign target was detasked on the United States. Collection was not removed from data repositories until the selector for a different target was detasked on but collection was not purged from the databases until

~~(S//SI//REL TO USA, FVEY)~~ Human error caused a delay in deleting one transcript from an NSA database. an NSA analyst submitted a purge request with the intent of deleting collection from He mistakenly believed that the request would effect purging was deleted from when the mistake was found.

(b)(1)
(b)(3)-P.L. 86-36

(U//~~FOUO~~) Unintentional dissemination of U.S. identities.

(b)(1)
(b)(3)-P.L. 86-36

~~(S//SI//REL TO USA, FVEY)~~ During 2008, [redacted] SIGINT products were cancelled because they contained the identities of U.S. persons, organizations, or entities. In all instances, the reports were either not reissued or were reissued with proper minimization. Additionally there were [redacted] instances in which SIGINT analysts disseminated communications to, from, or about U.S. persons while pursuing foreign intelligence tasking. All data have been deleted or destroyed as required by USSID SP0018.

(b)(1)
(b)(3)-P.L. 86-36
(b)(3)-18 USC 798
(b)(3)-50 USC 3024(i)

~~(S//SI//NOFORN)~~ [redacted] an NSA/CSS field site learned from [redacted] was instructed to destroy the files. Destruction was confirmed on [redacted]

(b)(1)
(b)(3)-P.L. 86-36

~~(S//NF)~~ [redacted] information about a U.S. person was posted on INTELINK, which is a classified and highly secure intranet used by the U.S. Intelligence Community. A graphic containing a U.S. address was posted from [redacted] when the mistake was identified and corrected.

(b)(1)
(b)(3)-P.L. 86-36
(b)(3)-50 USC 3024(i)

~~(TS//SI//NF)~~ [redacted] during a review of intercept [redacted] an NSA/CSS analyst discovered that the [redacted] from a legitimate foreign target [redacted] in the United States from [redacted] The [redacted] was notified and destroyed the five intercepts for the timeframe the target was in the United States.

(b)(1)
(b)(3)-P.L. 86-36

~~(TS//REL TO USA, FVEY)~~ [redacted] an NSA/CSS analyst included unminimized SIGINT in the form of a [redacted] to a [redacted] customer. When this USSID SP0018 violation was discovered [redacted] the analyst and the customer destroyed the files. Minimized data was then forwarded to [redacted]

(b)(1)
(b)(3)-P.L. 86-36
(b)(3)-18 USC 798
(b)(3)-50 USC 3024(

~~(TS//REL TO USA, FVEY)~~ [redacted] an NSA/CSS analyst [redacted] When the error was found the same day, the [redacted] was destroyed. All [redacted] in development were reviewed for U.S. person information, and the analysts received remedial training.

~~(S//SI//REL)~~ [redacted] the name of a U.S. organization involved with the [redacted] was included in a tip to [redacted] without a finding that the U.S. identity was necessary to understand the foreign intelligence or assess its importance. The tip was recalled and the recipients destroyed their copies.

(b)(1)
(b)(3)-P.L. 86-36
(b)(3)-18 USC 798
(b)(3)-50 USC 3024(

(b)(1)
(b)(3)-P.L. 86-36

~~(S//SI//NF)~~ [redacted] an NSA analyst included information from SIGINT about a [redacted] in a facsimile to [redacted] although, within NSA, the [redacted] is not part of the SIGINT production chain. Additionally, the same unminimized and unevaluated traffic was forwarded to a [redacted] assigned to

(b)(1)
(b)(3)-P.L. 86-36
(b)(3)-18 USC 798
(b)(3)-P.L. 86-36

NSA. The [redacted] was not authorized to receive unminimized and unevaluated SIGINT. In both instances, the disseminated data was destroyed on [redacted] (b)(3)-P.L. 86

~~(TS//SI//NF)~~ Before obtaining U.S. identity release on [redacted] an NSA analyst e-mailed a briefing that included identities of a U.S. [redacted] and U.S. [redacted] to the [redacted] later that month. On [redacted] when the analyst recognized the mistake, she directed destruction of the brief by the [redacted] as she applied for an identity release [redacted] had no record of the e-mailed briefing to destroy.

(b)(1)
(b)(3)-P.L. 86-36

~~(S//SI//REL TO USA, FVEY)~~ [redacted] the name of a U.S. person was included in [redacted] e-mail tips to elements inside and outside the SIGINT Production Chain. The violation was recognized the same day. The e-mails were recalled and a destruction notification was forwarded to all addressees.

~~(TS//SI//REL TO USA, FVEY)~~ [redacted] an NSA analyst included [redacted] U.S. person [redacted] analysts. The NSA analyst forwarded [redacted] On [redacted] the analyst noticed that he had not minimized the U.S. identifiers. He directed and confirmed the destruction of the charts by [redacted]

(b)(1)
(b)(3)-P.L. 86-36
(b)(3)-18 USC 798
(b)(3)-50 USC 3024(i)

(U) Foreign Intelligence Surveillance Act (FISA) Activities

(b)(1)
(b)(3)-P.L. 86-36

~~(TS//SI//NF)~~ NSA incurred violations on [redacted] Foreign Intelligence Surveillance Court (FISC)-authorized targets in 2008. All collection has been terminated, and all intercepts have been deleted or destroyed as required by USSID SP0018.

~~(TS//SI//NF)~~ [redacted] procedural problems occurred [redacted] forwarded FISA data to unauthorized NSA [redacted] the receiving analysts immediately deleted the data and educated [redacted]

(b)(1)
(b)(3)-P.L. 86-36

~~(TS//SI//NF)~~ [redacted]

(b)(1)
(b)(3)-P.L. 86-36
(b)(3)-18 USC 798
(b)(3)-50 USC 3024(i)

~~(S//SI)~~ NSA retained [redacted] data longer than the retention period authorized by a FISC Order. Unaware that the retention period was a condition of the docket and not a technical limitation of the data management device, dataflow managers kept the data longer than the 30-day retention limitation set by the court. The data was sequestered on [redacted] and the court was notified. The FISC revised the order to match the natural retention periods of NSA systems.

(b)(1)
(b)(3)-P.L. 86-36
(b)(3)-50 USC 3024(i)

(b)(1)
(b)(3)-P.L. 86-36

~~(TS//SI//NF)~~ Additionally, [redacted] there were [redacted] incidents in which the targeting of foreign telephone numbers overseas resulted in collection of calls that originated from [redacted] When the call origination location was identified on those days, the intercept was deleted from the database. No reports were issued.

(b)(1)
(b)(3)-P.L. 86-36
(b)(3)-50 USC 3024(i)

~~(TS//SI//NF)~~ [redacted] an NSA analyst retained an inadvertently acquired communication of a U.S. official while targeting a FISC-authorized telephone number. The U.S. person had been called from the targeted number [redacted] The transcript and associated voice intercept were deleted from the database and the data management system on [redacted] when the violation was recognized.

(b)(1)
(b)(3)-P.L. 86-36

~~(TS//SI//NF)~~ [redacted] an NSA team leader discovered that a target [redacted] in the United States [redacted] The query and resulting collection was deleted the same day.

(b)(1)
(b)(3)-P.L. 86-36
(b)(3)-50 USC 3024(i)

~~(TS//SI//NF)~~ [redacted] an NSA/CSS field analyst tipped information on [redacted] intercepts to other SIGINT analysts using a communication tool that was not authorized as a dissemination tool for [redacted] data because it does not have [redacted] When the problem was recognized on [redacted] the data was deleted. Although not a violation of the FISA and related authorities, the practice does not provide an audit trail of U.S. person information passed to others within the SIGINT production chain. The process for using [redacted] was amended [redacted]

(b)(1)
(b)(3)-P.L. 86-36

~~(TS//SI//NF)~~ [redacted] an NSA/CSS analyst discovered a FISC-authorized selector associated with a foreign [redacted] had not been removed from tasking on [redacted] Pursuant to the FISC order, detasking [redacted] However, a problem with the collection system [redacted] prevented the execution of the action. When the system problem was rectified on [redacted] a review of target selectors was conducted. [redacted] additional selectors affected by the system problem were removed from tasking.

(b)(1)
(b)(3)-P.L. 86-36
(b)(3)-50 USC 3024(i)

~~(TS//SI//NF)~~ The identity of a U.S. person was not masked on [redacted] when a file on a FISC-authorized target [redacted] analyst recognized the oversight, deleted the file and notified NSA. The NSA/CSS analysts associated with the violation were retrained on FISA minimization.

(b)(1)
(b)(3)-P.L. 86-36
(b)(3)-50 USC 3024(i)

~~(TS//SI//NF)~~ [redacted] an NSA analyst learned that a telephone number had not been [redacted] because of a typing error. This mistake resulted in the collection of [redacted] from the United States between [redacted] Once identified, the typing error was corrected, and the [redacted] intercepts were deleted from the NSA database on [redacted]

(b)(1)
(b)(3)-P.L. 86-36
(b)(3)-18 USC 798
(b)(3)-50 USC 3024(i)

~~(TS//SI//NF)~~

~~(TS//SI//NF)~~ NSA analysts queried a total of telephone selectors that had not been vetted as Although authorized to query telephone business records data directly, analysts The FISA business records queries require reasonable suspicion determination. This misperception was corrected through instruction. Search results were not retained by the analysts, and no reports were issued. This mistake has resulted in increased internal controls

(b)(1)
(b)(3)-P.L. 86-36

L. 86-36
(b)(3)-50 USC 3024(i)

~~(TS//SI//NF)~~ Human error resulted in the targeting of e-mail selectors Although the selectors were removed NSA analysts did not annotate that the selectors were terminated Consequently, the selectors remained active All collection related to the targets was destroyed, and no reports were issued.

~~(TS//SI//NF)~~ Another human error resulted in the targeting of e-mail selectors from Although the selectors were removed from NSA analysts did not annotate that the selectors were terminated Consequently, the selectors remained active All collection related to the targets was destroyed, and no reports were issued.

(b)(1)
(b)(3)-P.L. 86-36

~~(S//SI//REL TO USA, FVEY)~~ an NSA analyst e-mailed FISA-authorized collection data to who was not authorized to receive the FISA data. U.S. person information was not included in the e-mail. The NSA analyst, who misunderstood information sharing policy, confirmed the destruction of the data by the on

(U//~~FOUO~~) Business Record FISA (BRFISA)

~~(TS//SI//REL TO USA, FVEY)~~ an NSA analyst accessed BRFISA data for without authorization. The violation occurred because the analyst The analyst updated the navigation software on and other analysts were reminded to update their software. No data was retained, and no reports were issued.

~~(TS//SI//REL TO USA, FVEY)~~ passed a mistyped phone number to an NSA analyst The one digit change resulted in the targeting of an number in BRFISA data from All related call

chaining results were purged on and

~~(TS//SI//NF)~~ an NSA analyst improperly accessed BRFISA data for a U.S. telephone number. Although the number was associated with a foreign target, it had not been approved for call chaining in the BRFISA data. The analyst did not know that approval must be sought for BRFISA call chaining. No data was retained, and no reports were issued.

~~(S//SI//NF)~~ **The Protect America Act of 2007 (PAA).** There were PAA incidents in 2008. In of the incidents, e-mail addresses belonging to legitimate foreign targets, whose foreignness was confirmed at tasking, were active in the United States.

~~(TS//SI//REL TO USA, FVEY)~~ On occasions, NSA analysts tasked e-mail selectors that had been incorrectly typed. Tasked the selectors were invalid and no collection resulted. The selectors were removed when the mistakes were recognized on an NSA analyst learned that he had tasked a target's old e-mail address on There was no collection on that selector, and it was removed from tasking on

(b)(1)
(b)(3)-P.L. 86-36

~~(TS//SI//REL TO USA, FVEY)~~ an e-mail selector that did not belong to the intended target was tasked because of a typing error. The location of the tasked e-mail address is not known. No collection occurred from when the mistake was identified.

~~(TS//SI//NF)~~ Human error led to the targeting of an individual while he was in the United States Although the target selectors were during the visit, intercepts were deleted from the database and data management system when the violation was identified on No reporting resulted from the collection.

~~(TS//SI//NF)~~ Collection continued during a target's visit to the United States because of a file problem. Although the selector was the United States on intercepts collected were purged from the database when they were identified on System checks have been implemented to prevent the problem from recurring.

(b)(1)
(b)(3)-P L. 86-36
(b)(3)-18 USC 798

~~(TS//SI//REL TO USA, FVEY)~~ a translation mistake resulted in collection on a target while he was in the United States.

The violation was recognized on The resulting intercepts were deleted from the database and the voice management system on The selector was also removed the same day.

(b)(1)
(b)(3)-P.L. 86-36
(b)(3)-18 USC 798
(b)(3)-50 USC 3024(i)

~~(TS//SI//NF)~~ A targeted e-mail selector [redacted] the United States [redacted] The analyst wrongly assumed the target was located outside the United States. [redacted] The selector was detasked on [redacted] No collection occurred.

(b)(1)
(b)(3)-P.L. 86-36

~~(S//SI//NF)~~ On [redacted] occasions, NSA/CSS analysts did not purge PAA-related collection from NSA databases in a timely manner. [redacted] an e-mail selector of a legitimate foreign target was detasked because [redacted] Although the database purging began [redacted] collection from the [redacted] databases was not removed until [redacted] another target selector was detasked, but the purging of four databases was not completed until [redacted] Lastly, [redacted] a target selector was detasked, but the data was not completely purged from the [redacted] databases until [redacted]

~~(TS//SI//NF)~~ [redacted]

(b)(1)
(b)(3)-P.L. 86-36
(b)(3)-18 USC 798

(b)(1)
(b)(3)-P.L. 86-36

~~(TS//SI//NF)~~ NSA failed to remove a target selector from tasking when [redacted] Research revealed that [redacted] the United States on [redacted] The selector was detasked on [redacted] No collection occurred.

(b)(1)
(b)(3)-P.L. 86-36
(b)(3)-18 USC 798
(b)(3)-50 USC 3024(i)

~~(TS//SI//REL TO USA, FVEY)~~ During a tasking record review, NSA learned that [redacted] targeted selectors had been tasked under the wrong PAA authority. This due diligence measure found that analysts had mistakenly selected PAA Certification [redacted] instead of [redacted] The [redacted] errors occurred from [redacted] with no resulting collection. The [redacted] occurred from [redacted] The associated intercept was purged from NSA databases on [redacted]

(b)(1)
(b)(3)-P.L. 86-36

~~(TS//SI//REL TO USA, FVEY)~~ A selector was tasked on [redacted] and detasked the same day when the analyst recognized that the target location research had not been completed. [redacted] No collection occurred.

(b)(1)
(b)(3)-P.L. 86-36
(b)(3)-50 USC 3024(i)

~~(TS//SI//NF)~~ NSA failed to detask an AG-authorized selector from PAA collection when the FISA Amendments Act (FAA) was signed on 12 July 2008. An NSA analyst reviewing tasking files discovered the oversight on [redacted] The telephone number was detasked the same day. No collection occurred between [redacted]

~~(TS//SI//NF)~~ [redacted] NSA analysts learned that an e-mail address did not belong to the intended target. The [redacted] forwarded a mistyped e-mail address that was tasked under PAA

(b)(1)
(b)(3)-P.L. 86-36

Certification [redacted] The e-mail selector was detasked, and resulting collection was purged from NSA databases [redacted]

~~(TS//SI//NF)~~ [redacted] NSA analysts learned that a target's e-mail selector [redacted] The selector was detasked [redacted] and collection was purged from NSA databases [redacted]

(b)(1)
(b)(3)-P.L. 86-36

~~(TS//SI//REL TO USA, FVEY)~~ During a tasking record review on [redacted] NSA analysts learned that a targeted selector had been tasked under the wrong authority. This due diligence found that the analyst mistakenly selected FAA [redacted] Certification instead of the FAA [redacted] Certification. No collection occurred between [redacted] when the selectors were tasked and [redacted] when the selector was detasked, and no reports were issued.

(b)(1)
(b)(3)-P.L. 86-36
(b)(3)-50 USC 3024(i)

~~(S//SI//NF)~~ **Update.** In the NSA/CSS report ending 31 December 2007, NSA reported one instance in which a valid target was incorrectly tasked from [redacted] Further analysis of the incident revealed that the target's location outside the United States was verified according to approved procedures at the time of tasking, and there was no change in the target's location [redacted]

(b)(1)
(b)(3)-P.L. 86-36

~~(TS//SI//REL TO USA, FVEY)~~ **The FISA Amendments Act.** There were [redacted] FAA incidents in 2008.

~~(TS//SI//REL TO USA, FVEY)~~ [redacted] an NSA analyst forwarded FAA data to recipients who were not cleared for FAA. The analyst intended to send the e-mail to cleared [redacted] analysts but selected an e-mail alias with a broader [redacted] audience. The e-mail was recalled and destroyed on [redacted]

~~(TS//SI//NF)~~ [redacted]

1)
3)-P.L. 86-36
3)-18 USC 798
3)-50 USC 3024(i)

(b)(1)
(b)(3)-P.L. 86-36

~~(TS//SI//REL TO USA, FVEY)~~ During a tasking record review on [redacted] NSA analysts learned that [redacted] targeted selectors had been tasked under the wrong authority. This due diligence found that the analyst mistakenly selected PAA Certification [redacted] instead of the FAA

(b)(1)
(b)(3)-P.L. 86-36
(b)(3)-50 USC 3024(i)

(b)(1)
(b)(3)-P.L. 86-36
(b)(3)-50 USC 3024(i)

(b)(1)
(b)(3)-P.L. 86-36
(b)(3)-18 USC 798
(b)(3)-50 USC 3024(i)

[redacted] Certification. No collection occurred between [redacted] when the selectors were tasked and [redacted] when the correct authorization was assigned.

~~(TS//SI//NF)~~ [redacted] NSA analysts learned that a target's e-mail selector [redacted] but his selector was missed when other selectors were detasked. The selector was detasked [redacted] and collection was purged from NSA databases on [redacted]

(b)(1)
(b)(3)-P.L. 86-36

~~(TS//SI//NF)~~ A valid foreign FAA target traveled to the United States and [redacted] The analyst submitted a detasking request [redacted] but the detasking did not take effect [redacted] NSA databases were purged of collection on [redacted]

~~(S//SI//NF)~~ A target selector was not detasked during a target's [redacted] visit to the United States. [redacted] an NSA analyst requested detasking of the target's e-mail selector on [redacted] The selector was removed [redacted] but the analyst responsible for [redacted] detasking process inadvertently omitted the request [redacted]

(b)(1)
(b)(3)-P.L. 86-36
(b)(3)-50 USC 3024(i)

[redacted] Resulting collection was purged from NSA databases. No reporting occurred.

(b)(1)
(b)(3)-P.L. 86-36

~~(TS//SI//REL TO USA, FVEY)~~ A target with U.S. and [redacted] citizenship was incorrectly tasked under the FAA [redacted] Certification [redacted] in violation of FAA Section 702. A U.S. person may not be tasked under the [redacted] Certification. The NSA analyst did not notice the target's dual citizenship when the e-mail selector was tasked. Resulting collection was purged from [redacted] NSA databases [redacted] A software processing error prevented the deletion of the data [redacted]

(b)(1)
(b)(3)-P.L. 86-36

~~(TS//SI//NF)~~ [redacted] an FAA-authorized target was using an e-mail address [redacted] Collection was purged from [redacted] NSA databases on [redacted] but a software processing error prevented the deletion of the data from [redacted] The problem was isolated [redacted] and the data was purged from the [redacted] To ensure no other purging requests were affected, the system administrators re-processed all purging requests dating back to [redacted]

~~(TS//SI//NF)~~ [redacted] an FAA-tasked e-mail account associated with an [redacted] from the United States. The selector was not detasked until [redacted] because of a database software problem, which was corrected on [redacted] The target selector to be detasked was in the processing backlog. Related collection was purged from NSA databases [redacted] No reporting occurred.

(b)(1)
(b)(3)-P.L. 86-36
(b)(3)-18 USC 798
(b)(3)-50 USC 3024(i)

(b)(1)
(b)(3)-P.L. 86-36

(b)(1)
(b)(3)-P.L. 86-36

~~(TS//SI//REL TO USA, FVEY)~~ NSA analysts learned on [redacted] that a target selector was not [redacted] the United States [redacted] an NSA analyst requested detasking of the target's e-mail selector on [redacted] The analyst submitted the detasking request, but failed to notify the detasking office of [redacted] Resulting collection was purged from the NSA databases on [redacted] No reporting occurred.

~~(TS//SI//NF)~~ [redacted] an e-mail selector was tasked for collection under the FAA [redacted] Certificate, although the target did not meet the FAA tasking standards. The error was identified on [redacted] and the selector was detasked on [redacted] The tasking process has been changed to reduce the risk of future mistakes. Applicable selectors are now [redacted] No collection or reporting occurred.

(b)(1)
(b)(3)-P.L. 86-36

~~(TS//SI//REL TO USA, FVEY)~~ Human error resulted in collection of a target while he was in the United States from [redacted] The second error occurred when a [redacted] analyst used an outdated target list [redacted] The list noted the target as outside the United States. [redacted] All related collection was purged from NSA databases on [redacted]

(b)(1)
(b)(3)-P.L. 86-36

~~(S//SI//NF)~~ [redacted] an NSA analyst [redacted] the United States, but failed to remove the [redacted] tasking for the target's e-mail selector. The process failure was corrected on [redacted] when the oversight was identified. Collection was purged from NSA databases on [redacted]

~~(TS//SI//NF)~~ [redacted]

(b)(1)
(b)(3)-P.L. 86-36

~~(TS//SI//REL TO USA, FVEY)~~ Human error caused a three-day detasking delay, which resulted in collection while the target [redacted] the United States. The request to terminate the FAA-authorized collection was submitted on [redacted] but was not completed until [redacted] The analyst left on Friday and did not return until Monday, at which time the selector was detasked, and the resulting collection was purged from a NSA database on [redacted] No reporting occurred on the unauthorized collection.

(b)(1)
(b)(3)-P.L. 86-36

(b)(1)
(b)(3)-P.L. 86-36
(b)(3)-18 USC 798
(b)(3)-50 USC 3024(i)

~~(TS//SI//REL TO USA, FVEY)~~ **Computer Network Exploitation.**

~~(TS//SI//REL TO USA, FVEY)~~

(b)(1)
(b)(3)-P.L. 86-36

(b)(1)
(b)(3)-P.L. 86-36
(b)(3)-18 USC 798
(b)(3)-50 USC 3024(i)

~~(TS//SI//NF)~~

~~(TS//SI//REL TO USA, FVEY)~~

(b)(1)
86-36
SC 798
SC 3024(i)

~~(TS//SI//NF)~~

~~(TS//SI//NF)~~

L. 86-36
USC 798
USC 3024(i)

~~(TS//SI//REL TO USA, FVEY)~~

(b)(1)
(b)(3)-P.L. 86-36

(b)(1)
(b)(3)-P.L. 86-36
(b)(3)-18 USC 798
(b)(3)-50 USC 3024(i)

(U) Counterintelligence Activities

(U) Nothing to report.

(b)(1)
(b)(3)-P.L. 86-36
(b)(3)-50 USC 3024(i)

(U) Intelligence-related Activities

~~(TS//SI//REL TO USA, FVEY)~~ From [redacted] was inappropriately forwarded to [redacted] NSA [redacted] analysts [redacted] failed to follow NSA policy and guidance for dissemination of SIGINT technical information and sent the data to the non-SIGINT analysts. The recipients destroyed the data on [redacted]

2. (U//~~FOUO~~) NSA OIG Intelligence Oversight Inspections, Investigations, and Special Studies.

(b)(1)
(b)(3)-P.L. 86-36

(U) **Intelligence Oversight Inspections**

(U//~~FOUO~~) During 2008, the Office of Inspector General (OIG) reviewed various intelligence NSA/CSS activities to determine whether they were conducted in accordance with applicable statutes, Executive Orders, AG procedures, and Department of Defense and internal directives. With few exceptions, the problems uncovered were routine and showed that operating elements understand the restrictions on NSA/CSS activities. The NSA/CSS Inspector General will track corrective actions through implementation.

(U//~~FOUO~~) **NSA/CSS Hawaii.** No questionable intelligence activities were discovered incident to the inspection. A survey of the workforce within and outside SIGINT operations revealed a general lack of understanding of SIGINT collection, minimization, and dissemination, but a good grasp of the restrictions related to data repository searches. The inspection found non-compliance in the completion of initial and annual refresher intelligence oversight training. The database to track training for those with access to SIGINT databases and their auditors was not accurate. Annual refresher training was 69.5 percent complete. A highlight of the inspection was the [redacted] database and Standard Operating Procedure (SOP) developed by [redacted] section. The SOP has reduced the detasking time from [redacted] and has helped prevent collection violations.

(b)(1)
(b)(3)-P.L. 86-36

(U//~~FOUO~~) **NSA/CSS Colorado.** No questionable intelligence activities were discovered incident to the inspection. A survey of the workforce within and outside SIGINT operations revealed a good understanding of intelligence oversight authorities. Mission Operations employees displayed a good understanding of the intelligence oversight authorities in relation to collection, minimization, and dissemination. Although frequent intelligence oversight training is being accomplished, internal controls for oversight are lacking. The inspection found non-compliance in the completion of initial and annual refresher intelligence oversight training within the mandated timeframe, and non-compliance of intelligence oversight training for reservists and deployed employees. NSA/CSS Colorado lacked a process to track training for employees with access to NSA databases and had no processes to update the data.

(U//~~FOUO~~) [redacted] No questionable intelligence activities were discovered incident to the inspection. Despite a 98 percent intelligence oversight training compliance rate, the results of a workforce survey were mixed. Weakness was shown in key subjects such as the definition of a U.S. person and the handling of unminimized and unevaluated SIGINT. The inspection found that intelligence oversight roles and responsibilities were not clearly defined and intelligence oversight processes and procedures were not developed and documented. (b)(3)-P.L. 86-36

(U//~~FOUO~~) [redacted] No questionable intelligence activities were discovered incident to the inspection. Overall, there is generally a good understanding of the intelligence oversight authorities. A joint inspection found that the [redacted] would benefit from documented and communicated processes. The focus of the [redacted] intelligence oversight program has been E.O. 12333 training, but not local incident handling procedures. Intelligence oversight training for newcomers is at an 86 percent compliance rate, and over 99 percent for annual E.O. 12333 refresher training. Although collectors, analysts, and supervisors are aware of the restrictions on the collection, analysis, and dissemination of U.S. person information, local incident reporting standards and internal controls to track newcomer training and the use of sensitive NSA databases are needed. (b)(3)-P.L. 86-36

(U//~~FOUO~~) **NSA Office of** [redacted] No questionable intelligence activities were discovered incident to the inspection. A survey of the workforce within the office revealed that the analysts generally know who to contact with intelligence oversight questions. The organization had an intelligence oversight training compliance rate of over 93 percent. The inspection found that the intelligence oversight within NSA's Office of [redacted] is appropriately managed and compliant with standing regulations. (b)(3)-P.L. 86-36

(U) Intelligence Oversight Special Study

(b)(1)
(b)(3)-P.L. 86-36
(b)(3)-50 USC 3024(i)

~~(S//REL TO USA, FVEY)~~ **NSA** [redacted] On 26 September 2008, the NSA/CSS OIG completed a special study of the NSA [redacted] The objectives of the review were to identify authorities for the handling of data in [redacted] and to determine whether policies and procedures are in place and followed to ensure compliance with those authorities. We also reviewed system security practices related to [redacted] information systems. We found that the [redacted] is not in compliance with the NSA Associate Directorate for Security and Counterintelligence policies and procedures in three instances. Specifically, the [redacted] lacks an oversight board; required quarterly meetings with the NSA OGC do not occur; and executive reviews have not been conducted. The study also found that three auditing practices do not follow internal control standards; there are no procedures for auditing [redacted] queries; and oversight of [redacted] system security is lacking. The NSA/CSS OIG will track corrective action through completion.

(b)(3)-P.L. 86-36

(U) **Intelligence Oversight Investigation**

~~(S//SI//REL TO USA, FVEY)~~ **Alleged Unauthorized Disclosure of Classified Information and Misuse of the United States SIGINT System.** The NSA/CSS OIG reported alleged unauthorized disclosure of classified information and misuse of the United States SIGINT System last quarter. In May 2008, a Navy Cryptologist met with an uncleared Navy Family Readiness social worker and disclosed that he had used the SIGINT system to target his ex-wife and other family members. An OIG inquiry found no evidence to support the sailor's claim.

(b)(1)
(b)(3)-P.L. 86-36
(b)(3)-50 USC 3024(i)

3. (U) Substantive Intelligence Oversight Program Changes.

~~(S//SI//NF)~~ Practicing due diligence, NSA has improved internal controls to reduce the risk of unauthorized collection. As a preventative measure,

~~(TS//SI//NF)~~ NSA/CSS analysts found that e-mail selectors in 2008. In each case, the selectors were detasked. Collection occurred in of the instances; NSA databases were purged of the intercept. No reports were issued.

4. (U) Command level changes to published directives or policies concerning intelligence or intelligence-related activities.

(U) Nothing to report.

(b)(1)
(b)(3)-P.L. 86-36

(b)(1)
(b)(3)-P.L. 86-36
(b)(3)-50 USC 3024(i)